

PATENT ABSTRACTS OF JAPAN

(43)Date of publication of application : 06.06.1995

(51)Int.Cl.

G06F	9/06
G06F	9/06
G06F	9/06
G06F	9/445
G06F	9/45
G06F	11/34

(71)Applicant : FUJITSU LTD

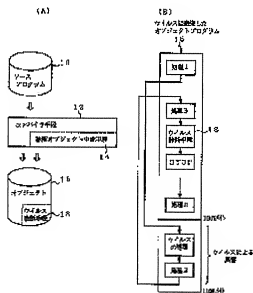
(72)Inventor : YAMAMOTO GOJI

(54) SYSTEM AND METHOD FOR PREPARING VIRUS DIAGNOSTIC MECHANISM AND VIRUS DIAGNOSTIC MECHANISM AND DIAGNOSTIC METHOD

(57)Abstract:

PURPOSE: To make it possible to diagnose virus infection by the OS of a computer or an object program itself to be executed as a program.

CONSTITUTION: When a source program 10 is converted into the object program 16 which is possible to be executed by a computer by a compile means 12, a virus diagnostic means 18 is generated in the object program 16 by a diagnosis object generation means 14 provided as one function of the compile means 12. The diagnostic means 18 performs the verification of the program size, the verification of a check sum, the verification of revision information on a preparation date month and year, etc., the verification of a disk address, the verification of an object program itself and the verification of the object program itself for which compression and restoration are utilized.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-146788

(43) 公開日 平成7年(1995)6月6日

(51) Int. Cl. ⁶	識別記号	片内整理番号	P 1	技術表示箇所
G 0 6 F 9/06	5 5 0 Z	9967-5B		
	4 1 0 P	9967-5B		
	5 3 0 A	9967-5B		
		9967-5B	G 0 6 F 9/06	4 2 0 S
		9202-5B	9/44	3 2 2 Z
審査請求 未請求 請求項の数36 ○L (全 17 頁) 最終頁に続く				

(21) 出願番号 特願平5-291658

(22) 出願日 平成5年(1993)11月22日

(71) 出願人 000009223

富士通株式会社

神奈川県川崎市中原区小田中1015番地

(72) 発明者 山本 剛司

神奈川県川崎市中原区小田中1015番地

富士通株式会社内

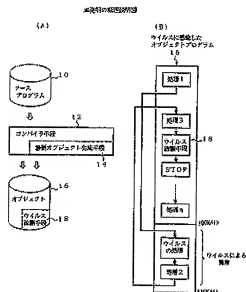
(74) 代理人 弁理士 竹内 進 (外 1 名)

(54) 【発明の名称】 ウイルス診断機構の作成システムと作成方法及びウイルス診断機構と診断方法

(57) 【要約】

【目的】 計算機のOS又はプログラムとして実行されるオブジェクトプログラム自身でウイルス感染を診断できるようにする。

【構成】 コンパイル手段12でソースプログラム10を計算機で実行可能なオブジェクトプログラム16に変換する際に、コンパイル手段12の1つの機能として設けられた診断オブジェクト生成手段14によって、オブジェクトプログラム16の中にウイルス診断手段18を生成する。ウイルス診断手段18は、プログラムサイズの検証、チェックサムの検証、作成年月日等のレビジョン情報の検証、ディスクアドレスの検証、オブジェクトプログラム自身の検証、圧縮復元を利用したオブジェクトプログラム自身の検証などを行う。



		(2)	特開平7-146788
	1	2	
	【特許請求の範囲】		
	【請求項1】 ソースプログラム(10)を計算機で実行可能なオブジェクトプログラム(16)に変換するコンパイラ手段(12)と、		
	前記コンパイラ手段(12)に設けられ、前記オブジェクトプログラム(16)の中にウイルス診断手段(18)を生成する診断オブジェクト生成手段(14)と、		
	を備えたことを特徴とするウイルス診断機構の作成システム。		
	【請求項2】 請求項1記載のウイルス診断機構の作成システムに於いて、前記診断オブジェクト生成手段(14)により生成された前記ウイルス診断手段(18)は、		
	前記コンパイラ手段(12)で変換された前記オブジェクトプログラム(16)のオリジナルサイズを格納したオリジナルサイズ格納手段と、		
	前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラム(16)のサイズを抽出する実行サイズ抽出手段と、		
	前記オリジナルサイズと前記実行時のサイズとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するサイズ判断手段と、を設けたことを特徴とするウイルス診断機構の作成システム。		
	【請求項3】 請求項1記載のウイルス診断機構の作成システムに於いて、前記診断オブジェクト生成手段(14)により生成された前記ウイルス診断手段(18)は、		
	前記コンパイラ手段(12)で変換された前記オブジェクトプログラム(16)のオリジナルのチェックサムを格納したオリジナルチェックサム格納手段と、		
	前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのチェックサムを抽出するチェックサム抽出手段と、		
	前記オリジナルチェックサムと前記実行時のチェックサムとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するチェックサム判断手段と、を設けたことを特徴とするウイルス診断機構の作成システム。		
	【請求項4】 請求項1記載のウイルス診断機構の作成システムに於いて、前記診断オブジェクト生成手段(14)により生成された前記ウイルス診断手段(18)は、		
	前記コンパイラ手段(12)で変換された前記オブジェクトプログラム(16)のオリジナルのレビジョン情報を格納したオリジナル・レビジョン格納手段と、		
	前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのレビジョン情報を抽出するレビジョン抽出手段と、		
	前記オリジナル・レビジョン情報と前記実行時のレビジョン情報とを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するレビジョン判断手段と、を設けたことを特徴とするウイルス診断機構の作成システム。		
	【請求項5】 請求項4記載のウイルス診断機構の作成システムに於いて、前記レビジョン判断手段は、更新を含む作成年月日、更新を含む作成時刻、作成者名、プログラム名、バージョン番号の少なくとも1つを用いたことを特徴とするウイルス診断機構の作成システム。		
	【請求項6】 請求項1記載のウイルス診断機構の作成システムに於いて、前記診断オブジェクト生成手段(14)により生成された前記ウイルス診断手段(18)は、		
	前記コンパイラ手段(12)で変換された前記オブジェクトプログラム(16)の格納先を示すディスクアドレスを格納したディスクアドレス格納手段と、		
	前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのディスクアドレスを抽出するディスクアドレス抽出手段と、		
	前記オリジナルのディスクアドレスと前記実行時のディスクアドレスとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するディスクアドレス比較手段と、を設けたことを特徴とするウイルス診断機構の作成システム。		
	【請求項7】 請求項1記載のウイルス診断機構の作成システムに於いて、前記診断オブジェクト生成手段(14)により生成された前記ウイルス診断手段(18)は、		
	前記コンパイラ手段(12)で変換された前記オブジェクトプログラム(16)をオリジナルとしてそのまま格納したオリジナル・オブジェクト格納手段と、		
	前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムを読み込む実行オブジェクト読込手段と、		
	前記オリジナル・オブジェクトと前記実行オブジェクトとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するオブジェクト比較手段と、を設けたことを特徴とするウイルス診断機構の作成システム。		
	【請求項8】 請求項1記載のウイルス診断機構の作成システムに於いて、前記診断オブジェクト生成手段(14)により生成された前記ウイルス診断手段(18)は、		
	前記コンパイラ手段(12)で変換された前記オブジェクトプログラム(16)のオリジナルを圧縮して格納した圧縮オブジェクト格納手段と、		
	前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムを読み込む実行オブジェクト読込手段と、		
	前記圧縮オブジェクト格納手段の圧縮オブジェクトプロ		

3

グラムを伸長して元に戻す復元手段と。

前記復元オブジェクトと前記実行オブジェクトとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するオブジェクト比較手段と、を設けたことを特徴とするウイルス診断機構の作成システム。

【請求項 9】請求項 2、3、4、5、6 又は 7 記載のウイルス診断機構の作成システムに於いて、前記診断オブジェクト生成手段（14）により生成された前記ウイルス診断手段（18）は、更に、前記オブジェクトプログラム（16）の実行によるプログラム自身の書き換えを

禁止する更新禁止手段を付加したことを特徴とするウイルス診断機構の作成システム。

【請求項 10】ソースプログラム（10）を計算機で実行可能なオブジェクトプログラム（18）に変換するコンパイル過程と、

前記コンパイル過程において、前記オブジェクトプログラム（16）の中にウイルス診断手段（18）を生成する診断オブジェクト生成過程と、を備えたことを特徴とするウイルス診断機構の作成方法。

【請求項 11】請求項 10 記載のウイルス診断機構の作成方法に於いて、前記診断オブジェクト生成過程で生成された前記ウイルス診断手段（18）は、前記コンパイル過程で変換された前記オブジェクトプログラム（16）のオリジナルサイズを格納するオリジナルサイズ格納過程と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのサイズを検出する実行サイズ検出過程と、

前記オリジナルサイズと前記実行時のサイズとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するサイズ判断過程と、を設けたことを特徴とするウイルス診断機構の作成方法。

【請求項 12】請求項 10 記載のウイルス診断機構の作成方法に於いて、前記診断オブジェクト生成過程で生成された前記ウイルス診断手段（18）は、前記コンパイル手段（12）で変換された前記オブジェクトプログラム（16）のオリジナルのチェックサムを格納したオリジナルチェックサム格納過程と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのチェックサムを検出するチェックサム検出過程と、

前記オリジナルチェックサムと前記実行時のチェックサムとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するチェックサム判断過程と、を設けたことを特徴とするウイルス診断機構の作成方法。

【請求項 13】請求項 10 記載のウイルス診断機構の作成方法に於いて、前記診断オブジェクト生成過程で生成された前記ウイルス診断手段（18）は、

前記コンパイル過程で変換された前記オブジェクトプロ

(3)

特開平 7-146788

4

グラム（16）のオリジナルのレビジョン情報を格納したオリジナル・レビジョン格納過程と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのレビジョン情報を検出するレビジョン検出過程と、

前記オリジナル・レビジョン情報と前記実行時のレビジョン情報とを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するレビジョン判断過程と、を設けたことを特徴とするウイルス診断機構の作成方法。

【請求項 14】請求項 13 記載のウイルス診断機構の作成方法に於いて、前記レビジョン情報として、更新を含む作成年月日、更新を含む作成時刻、作成者名、プログラム名、バージョン番号の少なくとも一つを用いたことを特徴するウイルス診断機構の作成方法。

【請求項 15】請求項 10 記載のウイルス診断機構の作成方法に於いて、前記診断オブジェクト生成過程で生成された前記ウイルス診断手段（18）は、前記コンパイル過程で変換された前記オブジェクトプログラム（16）の格納先を示すディスクアドレスを格納したディスクアドレス格納過程と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのディスクアドレスを検出するディスクアドレス検出過程と、

前記オリジナルのディスクアドレスと前記実行時のディスクアドレスとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するディスクアドレス比較過程と、を設けたことを特徴とするウイルス診断機構の作成方法。

【請求項 16】請求項 10 記載のウイルス診断機構の作成方法に於いて、前記診断オブジェクト生成過程で生成された前記ウイルス診断手段（18）は、前記コンパイル手段（12）で変換された前記オブジェクトプログラム（16）のオリジナルとしてそのまま格納したオリジナル・オブジェクト格納過程と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムを読込む実行オブジェクト読込過程と、

前記オリジナル・オブジェクトと前記実行オブジェクトとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するオブジェクト比較過程と、を設けたことを特徴とするウイルス診断機構の作成方法。

【請求項 17】請求項 10 記載のウイルス診断機構の作成システムに於いて、前記診断オブジェクト生成過程で生成された前記ウイルス診断手段（18）は、前記コンパイル過程で変換された前記オブジェクトプログラム（16）のオリジナルを圧縮して格納する圧縮オブジェクト格納過程と、

前記計算機でオペレーティングシステムまたはプログラ

59

(4)

特開平7-146788

5

6

ムとしてロードされた前記オブジェクトプログラムを読み込む実行オブジェクト読み込み手段と、前記圧縮オブジェクト格納手段の圧縮オブジェクトプログラムを伸長して元に戻す復元手段と、

前記復元オブジェクトと前記実行オブジェクトとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するオブジェクト比較手段と、を設けたことを特徴とするウイルス診断機構の作成方法。

【請求項18】請求項11、12、13、14、15、16又は17記載のウイルス診断機構の作成方法に於いて、前記診断オブジェクト生成過程で生成された前記ウイルス診断手段(18)は、更に、前記オブジェクトプログラム(16)の実行によるプログラム自身の書き換えを禁止する更新禁止過程を備えたことを特徴とするウイルス診断機構の作成方法。

【請求項19】計算機で実行可能な形式に変換されたオブジェクトプログラム(16)の中に、前記計算機のオペレーティングシステム又はプログラムの一部として実行されるウイルス診断手段(18)を設けたことを特徴とするウイルス診断機構。

【請求項20】請求項19記載のウイルス診断機構に於いて、前記ウイルス診断手段(18)は、前記コンパイル手段(12)で変換された前記オブジェクトプログラム(16)のオリジナルサイズを格納したオリジナルサイズ格納手段と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのサイズを抽出する実行サイズ抽出手段と、

前記オリジナルサイズと前記実行時のサイズとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するサイズ判断手段と、を設けたことを特徴とするウイルス診断機構。

【請求項21】請求項19記載のウイルス診断機構に於いて、前記ウイルス診断手段(18)は、前記コンパイル手段(12)で変換された前記オブジェクトプログラム(16)のオリジナルのチェックサムを格納したオリジナルチェックサム格納手段と、前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのチェックサムを抽出するチェックサム抽出手段と、

前記オリジナルチェックサムと前記実行時のチェックサムとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するチェックサム判断手段と、を設けたことを特徴とするウイルス診断機構。

【請求項22】請求項19記載のウイルス診断機構に於いて、前記ウイルス診断手段(18)は、前記コンパイル手段(12)で変換された前記オブジェクトプログラム(16)のオリジナルのレビジョン情報を格納したオリジナル・レビジョン格納手段と、

前記計算機でオペレーティングシステムまたはプログラ

ムとしてロードされた前記オブジェクトプログラムのレビジョン情報を抽出するレビジョン抽出手段と、

前記オリジナル・レビジョン情報と前記実行時のレビジョン情報とを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するレビジョン判断手段と、を設けたことを特徴とするウイルス診断機構。

【請求項23】請求項22記載のウイルス診断機構に於いて、前記レビジョン情報として、更新を含む作成年月日、更新を含む作成時刻、作成者名、プログラム名、バージョン番号の少なくとも1つを用いたことを特徴とするウイルス診断機構。

【請求項24】請求項19記載のウイルス診断機構に於いて、前記ウイルス診断手段(18)は、

前記コンパイル手段(12)で変換された前記オブジェクトプログラム(16)の格納先を示すディスクアドレスを格納したディスクアドレス格納手段と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのディスクアドレスを抽出するディスクアドレス抽出手段と、

前記オリジナルのディスクアドレスと前記実行時のディスクアドレスとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するディスクアドレス比較手段と、を設けたことを特徴とするウイルス診断機構。

【請求項25】請求項19記載のウイルス診断機構に於いて、前記ウイルス診断手段(18)は、

前記コンパイル手段(12)で変換された前記オブジェクトプログラム(16)のオリジナルとしてのそのまま格納したオリジナル・オブジェクト格納手段と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムを読み込む実行オブジェクト読み込み手段と、

前記オリジナル・オブジェクトと前記実行オブジェクトとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するオブジェクト比較手段と、を設けたことを特徴とするウイルス診断機構。

【請求項26】請求項19記載のウイルス診断機構に於いて、前記ウイルス診断手段(18)は、

前記コンパイル手段(12)で変換された前記オブジェクトプログラム(16)のオリジナルを圧縮して格納した圧縮オブジェクト格納手段と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムを読み込む実行オブジェクト読み込み手段と、前記圧縮オブジェクト格納手段の圧縮オブジェクトプログラムを伸長して元に戻す復元手段と、

前記復元オブジェクトと前記実行オブジェクトとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するオブジェクト比較手段と、を設けたこ

- 7
- とを特徴とするウイルス診断機構。
- 【請求項 2 7】請求項 2 0、2 1、2 2、2 3、2 4、2 5 又は 2 6 記載のウイルス診断機構に於いて、前記ウイルス診断手段（1 8）は、更に、前記オブジェクトプログラム（1 6）の実行によるプログラム自身の書き換えを禁止する更新禁止手段を付加したことを特徴とするウイルス診断機構。
- 【請求項 2 8】計算機で実行可能な形式に変換されたオブジェクトプログラム（1 6）の処理過程の中に、前記計算機の実行環境システム又はプログラムの一部として実行されるウイルス診断過程を設けたことを特徴とするウイルス診断方法。
- 【請求項 2 9】請求項 2 8 記載のウイルス診断方法に於いて、前記ウイルス診断過程は、前記コンパイル過程で変換された前記オブジェクトプログラム（1 6）のオリジナルサイズを格納するオリジナルサイズ格納過程と、前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのサイズを検出する実行サイズ検出過程と、前記オリジナルサイズと前記実行時のサイズとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するサイズ判断過程と、を設けたことを特徴とするウイルス診断方法。
- 【請求項 3 0】請求項 2 8 記載のウイルス診断方法に於いて、前記ウイルス診断過程は、前記コンパイル手段（1 2）で変換された前記オブジェクトプログラム（1 6）のオリジナルのチェックサムを格納したオリジナルチェックサム格納過程と、前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのチェックサムを検出するチェックサム検出過程と、前記オリジナルチェックサムと前記実行時のチェックサムとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するチェックサム判断過程と、を設けたことを特徴とするウイルス診断方法。
- 【請求項 3 1】請求項 2 8 記載のウイルス診断方法に於いて、前記ウイルス診断過程は、前記コンパイル過程で変換された前記オブジェクトプログラム（1 6）のオリジナルのレビジョン情報を格納したオリジナル・レビジョン格納過程と、前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのレビジョン情報を検出するレビジョン検出過程と、前記オリジナル・レビジョン情報と前記実行時のレビジョン情報とを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するレビジョン判断過程と、を設けたことを特徴とするウイルス診断機構の作成方法。
- 【請求項 3 2】請求項 3 1 記載のウイルス診断機構の作
- 50
- 成方法に於いて、前記レビジョン情報として、更新を含む作成年月日、更新を含む作成時刻、作成者名、プログラム名、バージョン番号の少なくとも 1 つを用いたことを特徴とするウイルス診断機構の作成方法。
- 【請求項 3 3】請求項 2 8 記載のウイルス診断方法に於いて、前記ウイルス診断過程は、前記コンパイル過程で変換された前記オブジェクトプログラム（1 6）の格納先を示すディスクアドレスを格納したディスクアドレス格納過程と、前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのディスクアドレスを検出するディスクアドレス検出過程と、前記オリジナルのディスクアドレスと前記実行時のディスクアドレス情報とを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するディスクアドレス比較過程と、を設けたことを特徴とするウイルス診断方法。
- 【請求項 3 4】請求項 2 8 記載のウイルス診断機構の作成方法に於いて、前記診断オブジェクト生成過程で生成された前記ウイルス診断手段（1 8）は、前記コンパイル手段（1 2）で変換された前記オブジェクトプログラム（1 6）のオリジナルとしてそのまま格納したオリジナル・オブジェクト格納過程と、前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムを読み込む実行オブジェクト読み込み過程と、前記オリジナル・オブジェクトと前記実行オブジェクトとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するオブジェクト比較過程と、を設けたことを特徴とするウイルス診断方法。
- 【請求項 3 5】請求項 2 8 記載のウイルス診断装置に於いて、前記ウイルス診断過程は、前記コンパイル過程で変換された前記オブジェクトプログラム（1 6）のオリジナルを圧縮して格納する圧縮オブジェクト格納過程と、前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムを読み込む実行オブジェクト読み込み過程と、前記圧縮オブジェクト格納過程の圧縮オブジェクトプログラムを伸長して元に戻す復元過程と、前記復元オブジェクトと前記実行オブジェクトとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するオブジェクト比較過程と、を設けたことを特徴とするウイルス診断方法。
- 【請求項 3 6】請求項 2 8、2 9、3 0、3 1、3 2、3 3、3 4 又は 3 5 記載のウイルス診断方法に於いて、前記ウイルス診断過程は、更に、前記オブジェクトプログラム（1 6）の実行によるプログラム自身の書き換えを禁止する更新禁止過程を備えたことを特徴とするウイルス

9

ルス診断方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、コンピュータウイルスの感染を予防するためウイルス診断機構の作成システムと作成方法並びにウイルス診断機構と診断方法に関し、特に、ワクチンが侵入した際に抗体として機能するウイルス診断機構の作成システムと作成方法並びにウイルス診断機構と診断方法に関する。

【0002】

【従来の技術】 近年のコンピュータシステムにあっては、コンピュータウイルスの発生に伴い、ウイルスに感染しない機能が要求されている。従来、外部から侵入したコンピュータウイルスの感染によりファイル破壊などの異常が起る場合には、コンピュータウイルスの機能を無効化させるコンピュータワクチンなどを開発して提供することで、ウイルス感染を防止するようにしている。

【0003】

【発明が解決しようとする課題】 しかしながら、従来のコンピュータワクチンを用いたウイルスの感染防止にあっては、新型のウイルスが発生すると、ワクチンの開発にある程度の時間がかかるため、その間にウイルスに感染する恐れがあった。またウイルスに感染していても、ファイルが1つ消える程度の被害に気付くことはほとんどなく、ウイルス感染に気付くまでにファイル破壊などの被害が拡大してしまう問題があった。

【0004】 本発明の目的は、コンパイルによるオブジェクトプログラムへの組み込みでウイルス診断機構を自動的に生成し、OS又はプログラムとして実行されるオブジェクトプログラム自身でウイルス感染を診断できるようにしたウイルス診断機構の作成方法と装置並びにウイルス診断機構と診断方法を提供する。

【0005】

【課題を解決するための手段】 第1図は、本発明によるウイルス診断機構の作成システムを例にとった原理説明図である。本発明のウイルス診断機構の作成システムは、コンパイル手段12とその中に設けた診断オブジェクト生成手段14で構成される。コンパイル手段12は、ソースプログラム10を任意の計算機で実行可能なオブジェクトプログラム16に変換する。

【0006】 診断オブジェクト生成手段14は、コンパイル手段12の1つの機能として設けられ、オブジェクトプログラム16の中にウイルス診断手段18を生成する。診断オブジェクト生成手段14により生成されるウイルス診断手段18は、

○プログラムサイズの検証

○チェックサムの検証

○作成年月日等のレビジョン情報（改訂情報）の検証

○ディレクトリの検証

(6)

特開平7-146788

10

○オブジェクトプログラム自身の検証

○圧縮復元を利用したオブジェクトプログラム自身の検証

のいずれかの機能を実現する。

【0007】 【プログラムサイズの検証】 コンパイル手段12で変換されたオブジェクトプログラム16のオリジナルサイズを格納しておく。計算機でオペレーティングシステムまたはプログラムとしてロードして実行されたオブジェクトプログラム16の実行サイズを検出してオリジナルサイズと比較し、両者が一致した場合は処理を続行し、不一致の場合はウイルス感染と判断して処理を中断する。

【0008】 【チェックサムの検証】 コンパイル手段12で変換されたオブジェクトプログラム16のオリジナルのチェックサムを格納しておく。計算機でオペレーティングシステムまたはプログラムとしてロードして実行されたオブジェクトプログラムのチェックサムを検出してオリジナルチェックサムと比較し、両者が一致した場合は処理を続行し、不一致の場合はウイルス感染と判断して処理を中断する。

【0009】 【レビジョン情報（改訂情報）の検証】 コンパイル手段12で変換されたオブジェクトプログラム16のオリジナルのレビジョン情報を格納しておく。計算機でオペレーティングシステムまたはプログラムとしてロードして実行されたオブジェクトプログラムのレビジョン情報を検出してオリジナル・レビジョン情報と比較し、両者が一致した場合は処理を続行し、不一致の場合はウイルス感染と判断して処理を中断する。

【0010】 ここで、レビジョン情報としては、更新を含む作成年月日、更新を含む作成時刻、作成者名、プログラム名、バージョン番号の少なくとも一つを用いる。

【ディレクトリの検証】 コンパイル手段12で変換されたオブジェクトプログラム16の格納先を示すディレクトリを格納しておく。計算機でオペレーティングシステムまたはプログラムとしてロードして実行されたオブジェクトプログラムのディレクトリを検出し、オリジナルのディレクトリと比較し、両者が一致した場合は処理を続行し、不一致の場合はウイルスに感染したと判断して処理を中断する。

【オブジェクトプログラム自身の検証】 コンパイル手段12で変換されたオブジェクトプログラム16のオリジナルとしてそのまま格納しておく。計算機でオペレーティングシステムまたはプログラムとしてロードして実行された前記オブジェクトプログラムを送込んでオリジナル・オブジェクトと比較し、両者が一致した場合は処理を続行し、不一致の場合はウイルスに感染したと判断して処理を中断する。

【0011】 【圧縮復元を利用したオブジェクトプログラム自身の検証】 コンパイル手段12で変換されたオブジェクトプログラム16のオリジナルを圧縮して格納し

59

11

ておく。計算機でオペレーティングシステムまたはプログラムとしてロードして実行されたオブジェクトプログラムを読み込み、同時に圧縮オブジェクトプログラムを伸張して元に戻す。そして復元オブジェクトと実行オブジェクトとを比較し、両者が一致した場合は処理を続行し、不一致の場合はウイルスに感染したと判断して処理を中断する。

【0012】更に、オブジェクトプログラム16の実行によるプログラム自身の書き換えを禁止する更新禁止手段を、ワクチンとしてコンパイルの段階で付加するようにしてもよい。さらに本発明は、コンパイラ手段12の診断オブジェクト生成手段14で生成されたウイルス診断機構18、すなわちワクチン診断オブジェクトそのものを対象とする。

【0013】

【作用】本発明によれば、コンパイラを用いてソースプログラムからオブジェクトプログラムに変換するオブジェクト生成時に、オブジェクト生成時にしか判らない情報としてのウイルス診断機構を生成してオブジェクトに埋め込んでいる。このため、計算機のオペレーティングシステムまたはプログラムとしての実行で、ウイルスによってオブジェクトが書き換えられた場合、オブジェクト自身がもつウイルス診断機構によって書き換えられたことをオブジェクトが認識できる。

【0014】従って、オブジェクトがウイルスに感染した可能性があるとして判断した場合には、実行を中断し、ウイルスの被害を最小限に食い止めることが可能となる。

【0015】

【実施例】図2は本発明によるウイルス診断機構を埋め込んだオブジェクトプログラムの作成に使用されるコンパイラマシンのハードウェア構成を示している。図2において、主記憶装置200にはオペレーティングシステム(OS)が格納され、電源投入時にコンパイラを実行するプログラムが展開される。主記憶装置200に対しては主記憶制御装置202が接続される。主記憶制御装置202にはCPU204およびチャネルプロセッサ208が接続される。

【0016】CPU204は主記憶装置200に転送されたコンパイラプログラムに従って、ソースプログラムを計算機で実行可能なアセンブラ語や機械語で表現されたオブジェクトプログラム(目的プログラム)に変換するコンパイラを行う。チャネルプロセッサ206のチャネル装置208には、チャネルバス210を介して磁気ディスクユニットなどを用いたファイル装置220、230、250、260が接続される。

【0017】ファイル装置220にはコンパイルを行うソースプログラム10が格納されている。ファイル装置230にはコンパイルの処理過程ごとに生成される中間ファイル240が格納されている。ファイル装置250にはコンパイルが済んだウイルス診断機構付きのオブ

(7)

待開平7-146788

12

ジェクトプログラム16が格納されている。更にファイル装置260にはコンパイルの処理過程で生成されるシンボルテーブル270が格納されている。

【0018】勿論、チャネルプロセッサ206の他のチャネル装置には図示しないCRT、プリンタ、キーボードなどの他の入出力機器が接続される。図3は本発明によるウイルス診断機構付きのオブジェクトプログラムの生成過程の概略を示す。図3において、ソースプログラム10はCOBOL、FORTRANなどの適宜のプログラム言語を使用して作成され、ファイル装置によるファイル情報として適用される。

【0019】コンパイラ部12はソースプログラム10を入力し、対象となる計算機で実行可能なアセンブラ語や機械語で表現されたオブジェクトプログラムへの変換処理を行い、ファイル情報としてオブジェクトプログラム16を出力する。本発明においては、コンパイラ部12の中に診断オブジェクト生成部14が新たに設けられている。診断オブジェクト生成部14はコンパイラ部12でソースプログラム10のオブジェクトプログラム16への変換処理の際に、オブジェクトプログラム16の中にウイルス診断機構18を自動的に生成する。

【0020】このコンパイラ部12に設けた診断オブジェクト生成部14によるウイルス診断機構18の生成機能はソースプログラム10に依存しておらず、ソースプログラム10の内容の如何に関わらず、コンパイラ部12を通すことで自動的にオブジェクトプログラム16の中に埋め込まれることになる。従って、ソースプログラム10の作成段階では本発明のウイルス診断機構18を全く意識する必要はない。

【0021】図4は図3の診断オブジェクト生成部14を備えたコンパイラ部12の機能構成を示した説明図である。このコンパイラ部としての機能は、図2のCPU204によるプログラムの実行の形で実現される。図4において、コンパイラは語義解析処理部26、構文解析処理部30、中間コード生成部34、コード最適化部38、コード生成部44および診断オブジェクト生成部14で構成される。

【0022】語義解析部26にはソースプログラム10が入力される。語義解析処理部26、構文解析処理部30、中間コード生成部34およびコード最適化部38においては、中間ファイル28、32、36、42の各々が生成される。語義解析処理部26はCOBOLやFORTRANなどの所定のプログラミング言語で書かれたソースプログラム10を入力し、プログラム言語の語義を解析する。即ち、プログラミング言語で書かれたソースプログラム10をトークンと呼ばれる単位ごとに切り、その単語の正当性をチェックする。

【0023】このトークンの代表例はキーワード、演算子、変数名、定数、区切り記号などがある。語義解析部26は全てのソースプログラム10の語義の正当性をチ

59

13

エックした後に トークンの集合でなる中間ファイル 28 を出力し、次の語彙解析処理部 30 に引き渡す。

【0024】 構文解析処理部 30 は語彙解析処理部 26 で生成された中間ファイル 28 を入力し、ソースプログラム 10 が使用されているプログラミング言語の文法規則に合致しているか否かチェックする。文法規則に合致していればソースプログラム 10 を実行する手順を決め、同様に中間ファイル 32 として出力する。この構文解析処理部 30 による構文解析は、一般的には 2 つの機能を備えている。1 つの機能はソースプログラム 26 上の各トークンが文法的に正しい位置にあるか否かのチェックである。

【0025】 2 つ目の機能はソースプログラム 10 上の全トークンの存在意味を解析した後にこれらの実行手順を決め、その手続をトークンの流れやグループ化として表現することである。一般には各トークンの実行順序の分析結果を表現するのに木構造 (パースツリー) が使用される。中間コード生成部 34 は構文解析処理部 30 で作成された中間ファイル 32 の木構造 (パースツリー) を入力し、コンパイラがもっている固有の中間コードに変換し、中間ファイル 36 を出力する。代表的な中間コードとしては 3 オペランド方式が知られている。

【0026】 コード最適化部 38 は中間コード生成部 34 で得られた中間ファイル 36 の中間コードを入力し、ターゲットとなる計算機上で最も少ない容量で且つ最も早い速度で実行可能な中間言語に変換し、中間ファイル 42 を出力する。一般的な最適化の手法としては、ローカルな最適化とループの最適化がある。ローカルな最適化とは余分な命令を減らすことである。またループの最適化とはループを毎回実行するごとに同じ値を示す式があるような場合は、これを無条件にループの外に出し出して最初の 1 回だけを実行するような方法である。

【0027】 コード生成部 44 はコード最適化が済んだ中間ファイル 42 の中間コードまたは中間言語をコード生成部 44 に入力し、ターゲットとなる計算機の命令セットに変換する。これに加えて本発明にあつては、更に診断オブジェクト生成部 44 を設けており、コード生成部 44 より最終的な変換結果として得られたターゲットとなる計算機の命令セットの中に、更にウイルス診断機能 18 を構成する命令セットを加える。

【0028】 このため、診断オブジェクト生成部 44 により加えられるウイルス診断機能 18 は、ターゲット計算機の命令セットでなるアセンブラ語あるいは機械語で記述された状態で準備されている。勿論、ソースプログラムに用いたプログラミング言語やコンパイラにおける中間言語で表現されたウイルス診断機能を準備し、対応するコンパイラ過程の段階で変換プログラムの中に埋め込むようにしてもよい。

【0029】 診断オブジェクト生成部 44 によるオブジェクトプログラムの内のウイルス診断機能 18 の埋込

(8)

特開平 7-146788

14

みが済むと、ファイル情報としてオブジェクトプログラム 16 が出力される。このようにコンパイラでソースプログラム 10 から変換されたウイルス診断機能 18 を埋め込んだオブジェクトプログラム 16 は、フロッピーディスク、磁気テープなどの媒体、あるいはオンラインにより対象計算機の ROM やディスクユニットにプログラムファイルとして提供されることになる。

【0030】 図 5 は本発明によりソースプログラムの中に埋め込まれたウイルス診断機能 18 の第 1 実施例を示した機能ブロック図である。図 5 において、第 1 実施例のウイルス診断機能 18 はプログラムサイズ検出部 20、サイズ判断部 22 およびオリジナルサイズ格納部 24 で構成される。オリジナルサイズ格納部 24 には図 3、図 4 に示したように、コンパイラ部 12 でオブジェクトプログラム 16 を作成した際のプログラムサイズ、例えばバイト数が、診断オブジェクト生成部 14 によるウイルス診断機能 18 の生成時にセットされている。

【0031】 プログラムサイズ検出部 20 は、このウイルス診断機能 18 を備えたソースプログラムが計算機上の OS あるいはプログラムとして実行される段階で、プログラムがウイルス診断機能 18 の処理に達する際の起動入力を受け、ウイルス診断機能 18 が埋め込まれているオブジェクトプログラムのプログラムサイズが何バイトかを検出する。

【0032】 サイズ判断部 22 はプログラムサイズ検出部 20 より実行プログラムサイズが得られると、オリジナルサイズ格納部 24 のオリジナルサイズと比較する。実行プログラムサイズがオリジナルサイズに一致していれば、ウイルス感染によるプログラム破壊がないことから続行出力を生じ、オブジェクトプログラムの中のウイルス診断機能 18 の埋込みが一致に続く次のプログラム処理にリターンする。

【0033】 これに対し、実行プログラムサイズがオリジナルサイズに一致しなかった場合には、ウイルス感染により異常な処理が加わってオブジェクトプログラムのプログラムサイズが変化していることが判る。この場合にはウイルス感染したものと判断し、中断出力を生じ、それ以降のオブジェクトプログラムの実行を抑制する。勿論、オブジェクトプログラムの中断に伴い、オペレータコントロールなどに対しウイルス感染による処理中断のメッセージ出力を行う。

【0034】 図 6 は図 5 に示したウイルス診断機能 18 の第 1 実施例の処理動作を示している。図 6 において、オブジェクトプログラムの処理からウイルス診断機能の起動に移行すると、まずステップ S1 で、現在実行している自己のオブジェクトプログラムのサイズを検出する。

【0035】 続いてステップ S2 で、予め格納しているオリジナルサイズと比較して一致するか否かを判断し、一致すれば再び正常なオブジェクトプログラムの処理に展

59

15

る。一方、検出したプログラムサイズがオリジナルサイズに等しくなかった場合には、ウイルス感染によるプログラムサイズの変化と判断し、ステップS3で処理を中断する。

【0036】図7はコンピュータウイルスの感染処理の一例を示している。図7のウイルスの感染処理にあつては、まずステップS1でOSまたはプログラムの最後にウイルス自身をコピーし、続いてステップS2でOSまたはプログラムからウイルスを呼び出すために破綻する命令を自分の最後にコピーする。そしてステップS3でOSまたはプログラムからウイルスを呼び出すように修正する。図8は図7の感染処理を行うウイルスに感染したオブジェクトプログラムについて、感染前と感染後のプログラム構造を示している。

【0037】図8(A)は感染前のオブジェクトプログラム48を示し、オブジェクトプログラム48は処理ブロック50-1~50-nに分けられた処理1~処理nを順番に実行する構造をもっている。このようなオブジェクトプログラム48が図7のウイルスに感染すると、図8(B)の感染後のソースプログラム52のようにプログラム構造が変化する。

【0038】即ち、処理ブロック50-1の処理1に続いてウイルスが自分自身をコピーしたウイルス処理ブロック54を本来のソースプログラム48の後ろに加えられ、続いてウイルスにより破綻された処理ブロック52の処理2が加えられる。そして、再び元のソースプログラム48の処理ブロック53の処理3に属するようなプログラム構造を作る。その結果、オリジナルのソースプログラム48に対し、ウイルス感染による処理で増加領域60がソースプログラム48に加わるようになる。

【0039】図9は図5に示したウイルス診断機構18を埋め込んだ本発明のソースプログラムの感染前と感染後のプログラム構造を示している。まず図9(A)は感染前の本発明によるソースプログラム48を示しており、処理ブロック50-3と50-4で示される処理2と処理4の間にコンパイルの際に生成されたウイルス診断機構18が埋め込まれている。

【0040】このウイルス診断機構18を埋め込んだオブジェクトプログラム48のプログラムサイズは例えは100Kバイトであり、これがオリジナルサイズとして図5に示したオリジナルサイズ格納部24に予めセットされている。図9(A)のオブジェクトプログラム48がウイルスに感染すると、図9(B)に示すようにオブジェクトプログラム56となる。このオブジェクトプログラムは、元のオブジェクトプログラム48の最後にウイルス自身をコピーしたウイルス処理ブロック54が追加され、続いてウイルスを呼び出すために破綻する命令として処理ブロック50-3の処理2をセットする。そして、オブジェクトプログラム48の処理ブロック50-1の処理1からウイルスをコピーしたウイルス処理

(9)

待機中7-146788

16

ブロック54に至り、破綻対象となる処理ブロック52-2の処理2から再びオブジェクトプログラム48の処理ブロック50-3の処理3に戻るプログラム構造を作り出す。

【0041】このようなウイルスによる感染が処理ブロック50-2の処理2について行われると、感染前100Kバイトであったプログラムサイズが、感染により例えは10Kバイトの増加領域60が加わって110Kバイトのプログラムサイズに変化してしまう。このようなプログラムサイズの変化に対し、この例では処理ブロック50-3の処理3に続いて図5に示したウイルス診断機構18が設けられており、図6のフローチャートに従ったウイルス診断処理が実行される。

【0042】この場合、プログラムサイズがオリジナルの100Kバイトに対し110Kバイトと変化しているため、プログラムサイズの不一致からウイルスによる感染と判断され、ブロック58に進んでオブジェクトプログラムの処理を中断することができる。従って、これ以上、オブジェクトプログラムを実行してウイルスによる感染が広がってしまうことを防止できる。また処理を中断に伴ってオペレータコンソールにウイルス感染による処理中断のメッセージ出力をオブジェクトプログラムのプログラム名称や番号と共に行うことで、特定のプログラムやOSにウイルス感染が起きたことを通知することができる。

【0043】図10は本発明によるウイルス診断機構18の第2実施例を示した機能ブロック図である。図10において、第2実施例のウイルス診断機構18はチェックサム検出部62、チェックサム判断部64およびオリジナルチェックサム格納部66で構成される。

【0044】コンパイルから出力されたソースプログラムは、ソースプログラムを格納するROMなどのメモリ装置における所定サイズのメモリブロックごとにチェックサムを求められていることから、この段階で得られたチェックサムをオリジナルチェックサムとしてオリジナルチェックサム格納部66に格納している。図10のウイルス診断機構18を埋め込んだソースプログラムの実行により、前に位置する処理が終了して超動力を流れると、チェックサム検出部62でメモリブロック単位にチェックサムを検出し、チェックサム判断部64で対応するブロックのオリジナルチェックサムと比較する。

【0045】チェックサムが一致すれば実行出力を生じ、チェックサムが不一致であればウイルスによる感染と判断し、中断出力により処理を中断する。図11は図10のチェックサムを用いたウイルス診断機構18の処理動作を示す。図11において、まずステップS1でオブジェクトプログラムの先頭ブロックのチェックサムを検出し、ステップS2でオリジナルのチェックサムに等しいか否かチェックする。

【0046】等しければステップS3に進み、全プロ

59

17

(10)

特開平7-146788

クを終了していなければ次のブロックに進み、ステップS1のブロックのチェックサムの検出とステップS2のオリジナルチェックサムとの比較を全ブロック終了まで繰り返す。全ブロックについてチェックサムがオリジナルに等しければ、元のオブジェクトプログラムの処理にリターンする。一方、いずれかのブロックでチェックサムがオリジナルに不一致であった場合には、ステップS5に進み、ウイルスに感染したものと判断し、処理を中断する。

【0047】図12は本発明によるウイルス診断機構18の第3実施例を示した機能ブロック図であり、この実施例はソースプログラムのレビジョン情報を利用するようにしたことを特徴とする。図12において、第3実施例のウイルス診断機構18はレビジョン情報検出部68、レビジョン判断部70およびオリジナル・レビジョン情報格納部72で構成される。

【0048】通常、オブジェクトプログラムはプログラムの光頭エリアにバージョンアップなどの改訂の様子を示すためレビジョン領域を設けている。このレビジョン領域には作成年月日、作成時刻、作成者名、プログラム名、バージョン番号などが格納されている。またオブジェクトプログラムは、ディスクユニットのディスク媒体上ではファイルとして扱われることから、ディスク媒体上のファイルにあるレビジョン領域も含む。

【0049】そこで、ウイルス診断機構18のオリジナル・レビジョン情報格納部72にコンパイルで生成する際にオブジェクトプログラムの作成年月日（更新年月日を含む）74、作成時刻（更新時刻を含む）76、作成者名78、プログラム名80およびバージョン番号82などをオリジナル・レビジョン情報としてセットしておく。

【0050】このウイルス診断機構18を埋め込んだオブジェクトプログラムの実行の処理が終わって再起動力を受けると、レビジョン情報検出部68でソースプログラムのレビジョン領域から現在のレビジョン情報を検出してレビジョン判断部70に引き渡す。レビジョン判断部70は検出されたレビジョン情報とオリジナル・レビジョン情報格納部72の格納情報とを比較し、一致すれば実行出力を生じ、不一致であればウイルスに感染したものと判断し、中断出力を生ずる。

【0051】レビジョン判断部70におけるレビジョン情報の比較は、この実施例にあつては作成年月日74、作成時刻76、作成者名78、プログラム名80およびバージョン番号82の全てについて行われ、いずれか1つでも不一致であるとウイルスに感染したものと判断して中断出力を行う。尚、ウイルス診断に使用するレビジョン情報としては、作成年月日、作成時刻、作成者名、プログラム名、バージョン番号のいずれか1つであってもよい。また、これ以外のレビジョン情報についても同様の処理がある。

【0052】図13は図12のウイルス診断機構18の第3実施例の処理動作を示している。まずステップS1でオブジェクトプログラムのレビジョン領域の情報を検出し、ステップS2で、予めセットしているオリジナルのレビジョン情報に一致するか否かを判断し、一致すればリターンしてオブジェクトプログラムを続行し、不一致であればウイルスに感染したものと判断し、ステップS3で処理を中断する。

【0053】図14は本発明のウイルス診断機構18の第4実施例を示したもので、この実施例はディスクアドレスを用いるようにしたことを特徴とする。第3実施例のウイルス診断機構18はディスクアドレス検出部84、ディスクアドレス比較部86およびオリジナル・ディスクアドレス格納部88で構成される。

【0054】コンパイルにより作成されたオブジェクトプログラムは、ターゲットとなる計算機システムの入出力サブシステムを構築するディスクユニットに格納される。このため、オブジェクトプログラムには格納先を示すディスクアドレスとして例えばボリューム番号、ファイル番号およびトラックアドレスが記述されている。そこで、コンパイルでオブジェクトプログラムの中にウイルス診断機構18を生成して埋め込む際に、オリジナル・ディスクアドレス格納部88にソースプログラムの格納先となるディスクアドレスを示すボリューム番号90、ファイル番号92およびトラックアドレス94などを格納しておく。この場合のアドレスは、開始アドレス、終了アドレスあるいはオブジェクトプログラムの一連のアドレスのいずれであってもよい。

【0055】このウイルス診断機構18を埋め込んだオブジェクトプログラムの実行でウイルス診断機構18が起動入力を受けると、ディスクアドレス検出部84でオブジェクトプログラムに埋め込んで記述されているディスクアドレス、例えばボリューム番号、ファイル番号およびトラックアドレスを検出してディスクアドレス比較部86に引き渡す。

【0056】ディスクアドレス比較部はオリジナル・ディスクアドレス格納部88からオリジナルとしてのボリューム番号90、ファイル番号92およびトラックアドレス94を読み出し、ディスクアドレス検出部84からの検出情報とオリジナルのレビジョン情報とを比較する。検出情報とオリジナル情報と一致すればウイルスに感染していないものと判断して、オブジェクトプログラムを続けて処理する実行出力を生ずる。検出情報とオリジナル情報が不一致であればウイルスによる感染でディスクアドレスの部分破壊されたものと判断し、中断出力を生ずる。

【0057】図15は図14のウイルス診断機構18の第4実施例の処理動作を示している。まずステップS1でディスクアドレスを検出し、ステップS2でオリジナルアドレスとの一致、不一致を判断し、一致していれば通常処理にリターンし、不一致であればウイルスに感染

19

したものとして ステップS3で処理を中断する。図16は本発明によるウイルス診断機構18の第5実施例を示した機能ブロック図であり、この第5実施例においてはオブジェクトプログラム全体をオリジナルと比較してウイルス感染を判断するようにしたことを特徴とする。

【0058】第5実施例のウイルス診断機構18は実行オブジェクト読込部96、オブジェクト比較部98およびオリジナル・オブジェクト格納部100で構成され、オリジナル・オブジェクト格納部100にはオリジナルのオブジェクトプログラム102がそのまま格納されている。図17は図16に示した第5実施例のウイルス診断機構18の生成の様子を示している。

【0059】図17において、コンパイラ12に設けた診断オブジェクト生成部14は、オブジェクトファイル220に對する1回目の出力でウイルス診断機構18を埋め込んだオブジェクトプログラム16を格納する。続いて診断オブジェクト生成部14の機能により、ウイルス診断機構18を埋め込んでいないオブジェクトプログラム102を2回目出力にてオブジェクトファイル220に格納する。

【0060】ターゲットとなる計算機システム104に對しては、1回目出力したウイルス診断機構18を埋め込んだオブジェクトプログラム16がインシナルプログラムロード（IPL）され、OSまたはプログラムとして実行される。このOSまたはプログラムとしてのウイルス診断機構18付きのオブジェクトプログラム16の実行において、図16に示したウイルス診断機構18の処理が行われ、オリジナル・オブジェクト格納部100の機能によりオブジェクトファイル220に2回目出力されて格納されているオブジェクトプログラム102がオリジナルとして読み込まれて診断に使用される。

【0061】図18は図16に示した第5実施例のウイルス診断機構18の処理動作を示している。まずステップS1でメモリのワーク領域に現在実行しているオブジェクトプログラムを読み込んで開閉する。続いてステップS2で外部のファイル220などに格納している計算機システム104では使っていないオリジナルのオブジェクトプログラム102を同じくワーク領域に読み込んで開閉し、ステップS1で読み込んだ実行しているオブジェクトプログラムとの比較をコマンド単位に行う。ここでコマンド単位の比較は、変数については処理ごとに異なるから、比較対象から除外する。

【0062】このようなコマンド単位の比較でオリジナルと全て一致すればウイルスに感染していないものと判断してオブジェクトプログラムの処理にリターンする。一方、コマンド単位の比較でオリジナルと不一致が生じた場合にはウイルスに感染したものと判断し、ステップS3で処理を中断する。尚、第5実施例のウイルス診断機構18にあっては、図17に示したようにオブジェク

(11)

特開平7-146788

20

トプログラムのサイズが大きき場合にはプログラム全体の比較判断となるために診断処理に時間がかかることから、ウイルス診断機構18の起動は計算機システム104のアイドルルーチンを検出して空き時間に行うことが望ましい。勿論、サイズの小さいオブジェクトプログラムであればオブジェクトのプログラムの実行ごとに行ってもよい。

【0063】図19は本発明によるウイルス診断機構18の第6実施例を示した機能ブロック図である。この第6実施例はオブジェクトプログラム全体の比較判断を行うと同時に、比較判断に用いるオリジナル・オブジェクトプログラムを圧縮形式で出力し、比較判断の際に伸長して元のオブジェクトプログラムに復元することで行うようにしたことを特徴とする。

【0064】この第6実施例のウイルス診断機構18は実行オブジェクト読込部106、オブジェクト比較部108、圧縮オブジェクト格納部110および伸長部（復元部）114で構成される。圧縮オブジェクト格納部110には圧縮されたオブジェクトプログラム112が格納されている。図20は図19に示した第6実施例のウイルス診断機構18を生成の様子を示している。

【0065】コンパイラ12に設けた診断オブジェクト生成部14は、1回目の出力で図19のウイルス診断機構18を埋め込んだオブジェクトプログラム16をオブジェクトファイル220に格納する。続いて2回目の出力でウイルス診断機構18を埋め込んでいないオブジェクトプログラムを出力するが、この実施例にあっては診断オブジェクト生成部14に圧縮アルゴリズムが設けられており、オブジェクトプログラムを圧縮した後に出力して、オブジェクトファイル220に圧縮オブジェクトプログラム112として格納する。

【0066】診断オブジェクトプログラム生成部14による圧縮アルゴリズムとしては、例えば2進算術符号化アルゴリズムが使用され、オブジェクトプログラム16のサイズを元の2%程度まで圧縮することができる。従って、圧縮オブジェクトプログラム112の格納領域を大幅に低減することができる。オブジェクトファイル220に格納されたウイルス診断機構18が埋め込まれたオブジェクトプログラム16は、ターゲットとなる計算機システム104にインシナルプログラムロード（IPL）されてOSまたはプログラムとして実行される。

【0067】この計算機システム104におけるオブジェクトプログラム16の実行において、ウイルス診断機構18が起動するとオブジェクトファイル220に格納されている圧縮オブジェクトプログラム112を読み出し、伸長部114で伸長した後に、オブジェクト比較部108で、現在実行しているオブジェクトプログラムとの比較判断を行う。

【0068】圧縮オブジェクトプログラム112を伸長

50

21

(12)

特開平7-146788

22

する身長部114はウイルス診断機構18専用ではなく、計算機システム104がもっている伸張プログラムを利用して行うことが望ましい。図21は図19に示したウイルス診断機構18の第5実施例の処理動作を示す。

【0069】まずステップS1で圧縮オブジェクトプログラムを読み込み、ステップS2で圧縮オブジェクトプログラムを伸張して元のオリジナル・オブジェクトプログラムに展開する。このような圧縮オブジェクトプログラムの読み込みと元のオブジェクトプログラムへの伸張は、計算機システム104におけるメモリのワーク領域上で行われる。

【0070】続いてステップS3で、現在実行中のオブジェクトプログラムを同じくワーク領域に読み込む。続いてステップS4で、圧縮形式から復元したオリジナル・オブジェクトプログラムと実行オブジェクトプログラムを例えばコマンド単位に比較して、一致の有無を判断する。この場合も第5実施例と同様、コマンドに含まれる変数は判断対象から除外する。2つのオブジェクトプログラムが一致していればウイルスによる感染はないものとして、元のオブジェクトプログラムの処理にリターンする。

【0071】一方、コマンド単位の比較で不一致が疑われる場合にはウイルスによる感染と判断し、ステップS5に進んで処理を中断する。この第6実施例にあっても、オブジェクトプログラム全体の比較判断になることから、プログラムサイズが大きい場合にはウイルス診断処理に時間がかかるので、計算機システム104のアイドル状態で診断処理を行うことが望ましい。勿論、プログラムサイズが小さければ、オブジェクトプログラムの中でウイルス診断処理を行えばよい。

【0072】更に本発明の他の実施例として、以上説明した第1実施例から第6実施例のウイルス診断機構18に加え、図3に示したコンパイラ部12でオブジェクトプログラム16を出力する際に、オブジェクトプログラム16に更新不可属性をセットして出力させることが望ましい。即ち、オブジェクトプログラム16がウイルスに感染すると、図8、図9に示したように感染によりオブジェクトプログラムの書き換えが行われる。このようなウイルス感染による書き換えを禁止するため、コンパイラから出力する際に更新不可属性をセットしてオブジェクトプログラム16を出力しておく。このような更新不可属性のセットはオブジェクトプログラム16にウイルス感染を防ぐワクチンを注入した機能をもつ。

【0073】即ち、本発明によりオブジェクトプログラムの中にウイルス診断機構を埋め込むと同時に、必要ならば更新不可属性のセットなどのワクチンを設けておくこともウイルス感染による被害を防ぐためには望ましい。但し、更新不可属性のようなワクチンは特定のウイルスには利くが別のウイルスには効果が無い場合が多

く、予防的な意味で設けることになる。

【0074】

【発明の効果】以上説明してきたように本発明によれば、ウイルスの感染がオブジェクトプログラムに埋め込まれたウイルス診断機構により判別し、しかも感染が判別と処理を中断することから、ウイルス感染による被害を最小限に抑え、適切なウイルスの感染防止対策をとることができる。

【0075】また、オブジェクトプログラムに対するウイルス診断機構の埋込みはコンパイラに設けた診断オブジェクト生成機能によりコンパイル段階で自動的に行われる。このため、ソースプログラムの製造段階でウイルス診断機構を添付する必要がなく、ソースプログラムの製造工程に負担を与えない。

【0076】また全てのソースプログラムのコンパイルについてオブジェクトプログラムの中にウイルス診断機構が自動的に埋め込まれ、これによってターゲット計算機のOSやプログラムがウイルスに感染したことを早期に発見して、且つ被害の拡大を確実に防止できる。

【図面の簡単な説明】

【図1】本発明の原理説明図

【図2】本発明で用いるコンパイラのハードウェア構成図

【図3】本発明によるウイルス診断機構の生成を示した説明図

【図4】コンパイラの機能構成を示した説明図

【図5】本発明のウイルス診断機構の第1実施例を示したブロック図

【図6】図5の処理動作を示したフローチャート

【図7】ウイルス感染処理の一例を示したフローチャート

【図8】ウイルス感染前と感染後のプログラム構造を示した説明図

【図9】図5のウイルス診断機構によりウイルス感染が判断された場合のプログラム構造の説明図

【図10】本発明のウイルス診断機構の第2実施例を示したブロック図

【図11】図10の処理動作を示したフローチャート

【図12】本発明のウイルス診断機構の第3実施例を示したブロック図

【図13】図12の処理動作を示したフローチャート

【図14】本発明のウイルス診断機構の第4実施例を示したブロック図

【図15】図14の処理動作を示したフローチャート

【図16】本発明のウイルス診断機構の第5実施例を示したブロック図

【図17】図16のウイルス診断機構の生成と診断処理の説明図

【図18】図16の処理動作を示したフローチャート

【図19】本発明のウイルス診断機構の第6実施例を示

23

(13)

特開平7-146788

24

したブロック図

【図20】図19のウイルス診断機構の生成と診断処理の説明図

【図21】図19の処理動作を示したフローチャート

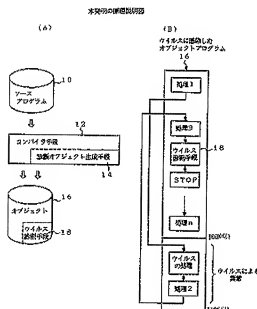
10: ソースプログラム
 12: コンパイラ部
 14: 診断オブジェクト生成部
 16: オブジェクトプログラム
 18: ウイルス診断機構
 20: プログラムサイズ検出部
 22: サイズ判断部
 24: オリジナルサイズ格納部
 26: 語彙解析処理部
 28、32、36、42: 中間ファイル
 30: 構文解析処理部
 38: コード最適化部
 44: コード生成部
 48: 感染前のオブジェクトプログラム
 52: 感染後のオブジェクトプログラム
 50-1~50-n: 処理ブロック
 54: ウイルスの処理ブロック
 56: 感染後の本発明のオブジェクトプログラム
 60: 感染による増加領域
 62: チェックサム検出部

*64: チェックサム判断部
 66: オリジナルチェックサム格納部
 68: レビジョン情報検出部
 70: レビジョン判断部
 72: オリジナル・レビジョン情報格納部
 84: ディスクアドレス検出部
 86: ディスクアドレス比較部
 88: オリジナル・ディスクアドレス格納部
 96、106: 実行オブジェクト読込部
 98、108: オブジェクト比較部
 100: オリジナル・オブジェクト格納部
 104: 計算機システム
 110: 圧縮オブジェクト格納部
 112: 圧縮オブジェクトプログラム
 114: 伸張部(復元部)
 200: 主記憶装置
 202: 主記憶制御装置
 204: CPU
 206: チャネル装置
 210: バイパス
 220、230、250、260: ファイル装置
 240: 中間ファイル
 270: シンボルテーブル

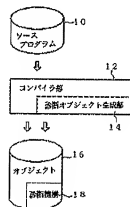
*

【図1】

【図3】



本発明によるウイルス診断機構の生成を示した説明図

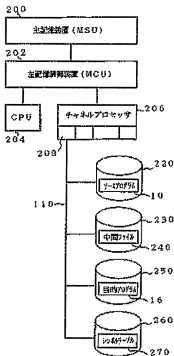


(14)

特開平 7-146788

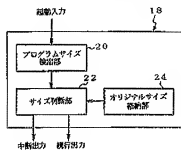
【図 2】

本発明で用いるコンピュータのハードウェア構成図



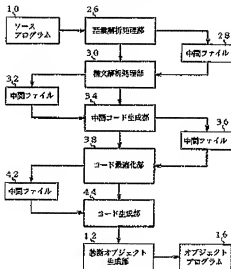
【図 5】

本発明のウイルス診断機構の第 1 実施例を示したブロック図



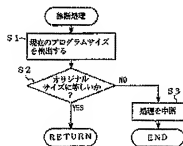
【図 4】

コンパイラの機能構成を示した説明図



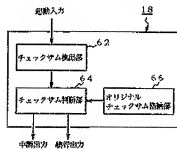
【図 6】

図 5 の処理動作を示したフローチャート



【図 10】

本発明のウイルス診断機構の第 2 実施例を示したブロック図

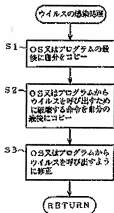


(15)

特開平 7-146788

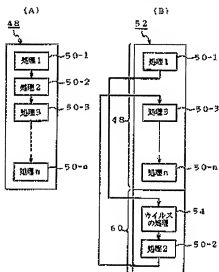
【図 7】

ウイルス感染処理の一例を示したフローチャート



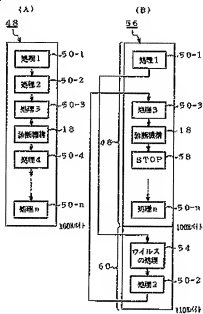
【図 8】

ウイルス感染前と感染後のプログラム構造を示した図解



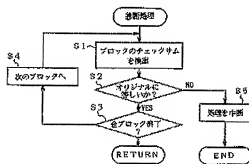
【図 9】

図5のウイルス診断機構によりウイルス感染が検出された場合のプログラム構造の例図



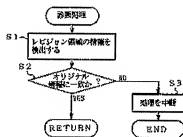
【図 11】

図10の処理動作を示したフローチャート



【図 13】

図12の処理動作を示したフローチャート

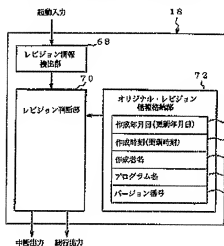


(15)

特開平 7-146788

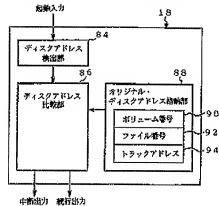
【図 12】

本発明のウイルス診断機構の第3実施例を示したブロック図



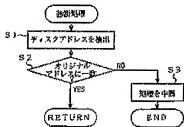
【図 14】

本発明のウイルス診断機構の第4実施例を示したブロック図



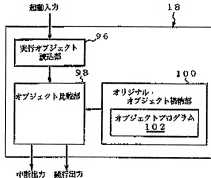
【図 15】

図 14 の処理動作を示したフローチャート



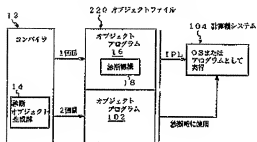
【図 16】

本発明のウイルス診断機構の第5実施例を示したブロック図



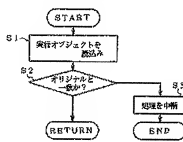
【図 17】

図 15 のウイルス診断機構の装置と診断部部の説明図



【図 18】

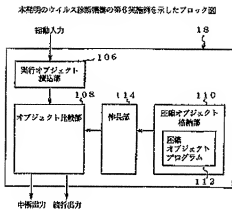
図 15 の処理動作を示したフローチャート



(17)

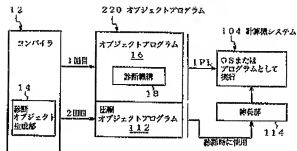
特開平 7-146788

【図 19】



【図 20】

図 19 のウイルス診断機構の生成と診断処理の説明図



フロントページの続き

(51)Int. Cl.^o

G 0 6 F 9/445

9/45

11/34

識別記号

片内整理番号

F I

技術表示箇所

A 5290-5B

【図 21】

図 19 の処理動作を示したフローチャート

